Bitcoin i inne kryptowaluty

Jakub Cisło

Programowanie z pasją

http://cislo.net.pl

jakub@cislo.net.pl

25 maja 2018

Plan wykładu

O czym będziemy mówić?

O czym będziemy mówić?

- Jak to działa?

O czym będziemy mówić?

- Jak to działa?
- Dlaczego to działa?

Wstęp

Co to kryptowaluta?

Co to kryptowaluta?

- krypto

Co to kryptowaluta?

- krypto - *kryptografia*

Co to kryptowaluta?

- krypto - *kryptografia*
- waluta

Co to kryptowaluta?

- krypto - *kryptografia*
- waluta

Przykłady:

Co to kryptowaluta?

- krypto - *kryptografia*
- waluta

Przykłady:

- Bitcoin

Co to kryptowaluta?

- krypto - *kryptografia*
- waluta

Przykłady:

- Bitcoin
- Ethereum

Co to kryptowaluta?

- krypto - *kryptografia*
- waluta

Przykłady:

- Bitcoin
- Ethereum
- Ripple

Co to kryptowaluta?

- krypto - *kryptografia*
- waluta

Przykłady:

- Bitcoin
- Ethereum
- Ripple
- Lite coin

Co to kryptowaluta?

- krypto - *kryptografia*
- waluta

Przykłady:

- Bitcoin
- Ethereum
- Ripple
- Lite coin
- Bitcoin cash

Hasz

Hasz

Mikołaj Kopernik

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar
- jednoznaczność

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar
- jednoznaczność
- szybkość obliczenia

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar
- jednoznaczność
- szybkość obliczenia
- losowość

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar
- jednoznaczność
- szybkość obliczenia
- losowość
- trudność odwrócenia

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar
- jednoznaczność
- szybkość obliczenia
- losowość
- trudność odwrócenia

Przykłady:

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar
- jednoznaczność
- szybkość obliczenia
- losowość
- trudność odwrócenia

Przykłady:

- MD4

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar
- jednoznaczność
- szybkość obliczenia
- losowość
- trudność odwrócenia

Przykłady:

- MD4
- MD5

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar
- jednoznaczność
- szybkość obliczenia
- losowość
- trudność odwrócenia

Przykłady:

- MD4
- MD5
- SHA256

Hasz

Mikołaj Kopernik

↓

`b94f18e6db30fb0fd75b9a1f5ea6946511017 68d953a43a4098e1804e9c0df13`

Własności:

- ustalony rozmiar
- jednoznaczność
- szybkość obliczenia
- losowość
- trudność odwrócenia

Przykłady:

- MD4
- MD5
- SHA256
- SHA512

Adres i portfel

Adres

Adres

`1HqAbUuE4k59YXxhfMxPbdyrkyd9LLoBAd`

Adres

`1HqAbUuE4k59YXxhfMxPbdyrkyd9LLoBAd`

klucz publiczny

Adres

`1HqAbUuE4k59YXxhfMxPbdyrkyd9LLoBAd`

klucz publiczny

`5K6iye9fsgn9cCsixMgYr3KterCofNhe8a6enVsXHy9nmXNpRqV`

Adres

`1HqAbUuE4k59YXxhfMxPbdyrkyd9LLoBAd`

klucz publiczny

`5K6iye9fsgn9cCsixMgYr3KterCofNhe8a6enVsXHy9nmXNpRqV`

klucz prywatny

Portfel

Portfel

Typy portfeli

Portfel

Typy portfeli

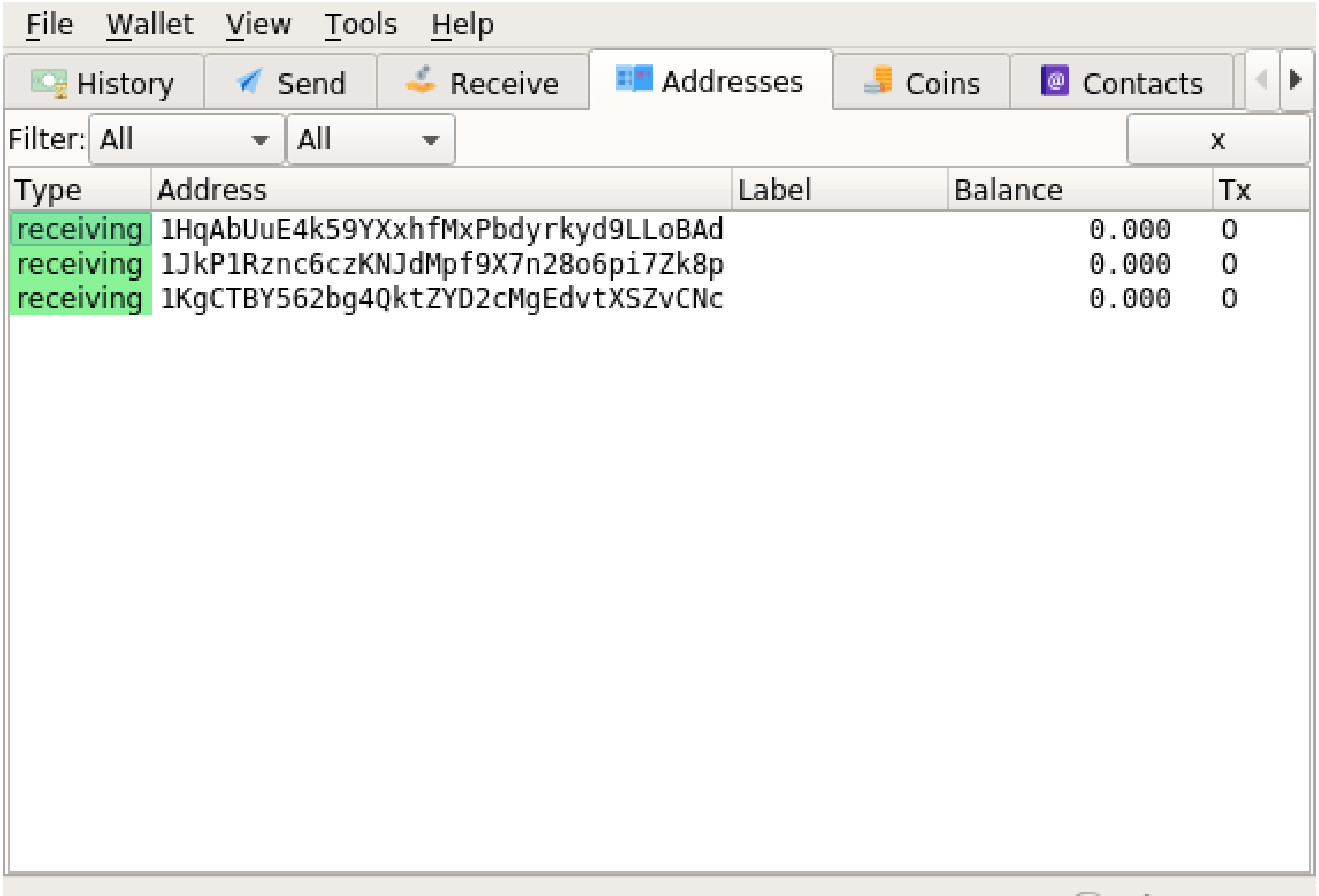
- aplikacja

Portfel

Typy portfeli

- aplikacja
- strona internetowa

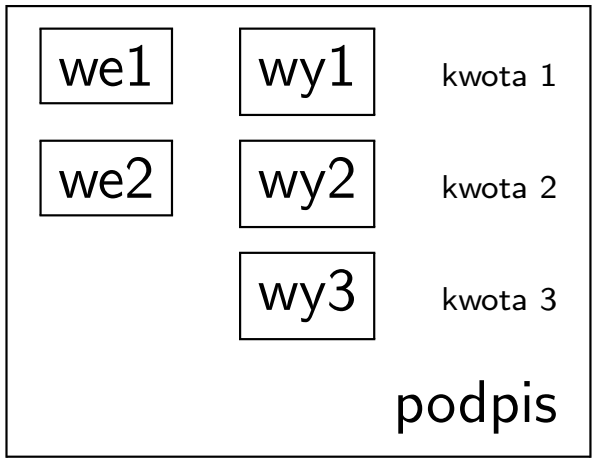
Electrum


File Wallet View Tools Help
History Send Receive Addresses Coins Contacts
Filter: All All x
Type Address Label Balance Tx
receiving 1HqAbUuE4k59YXxhfMxPbdyrkyd9LLoBAd 0.000 0
receiving 1JkP1Rznc6czKNJdMpf9X7n28o6pi7Zk8p 0.000 0
receiving 1KgCTBY562bg4QktZYD2cMgEdvtXSZvCNc 0.000 0

Blockchain

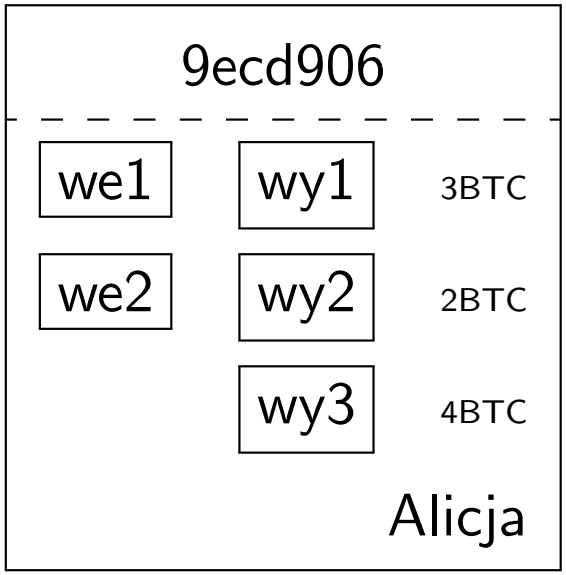
Transakcja

Transakcja

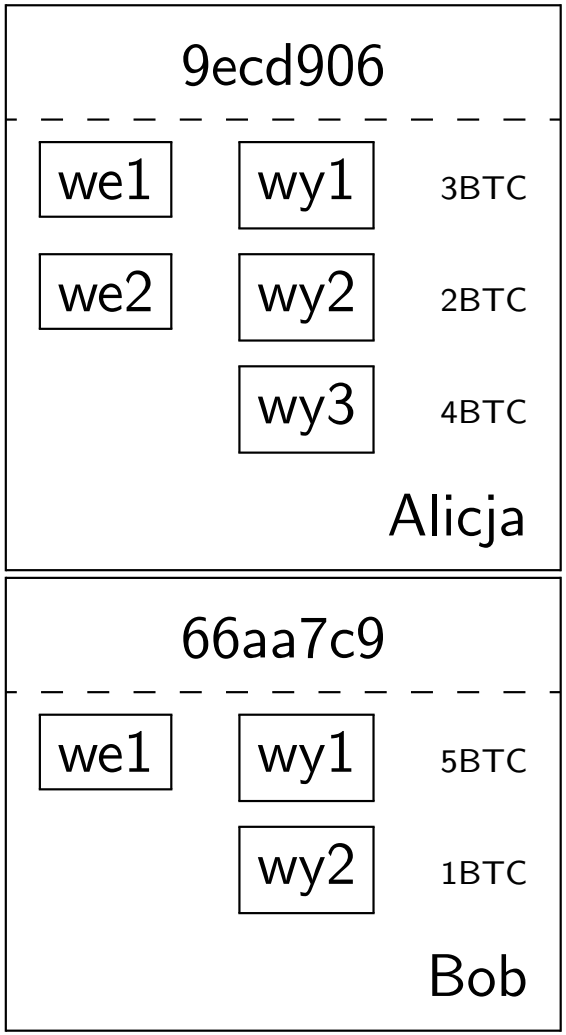


Transakcje

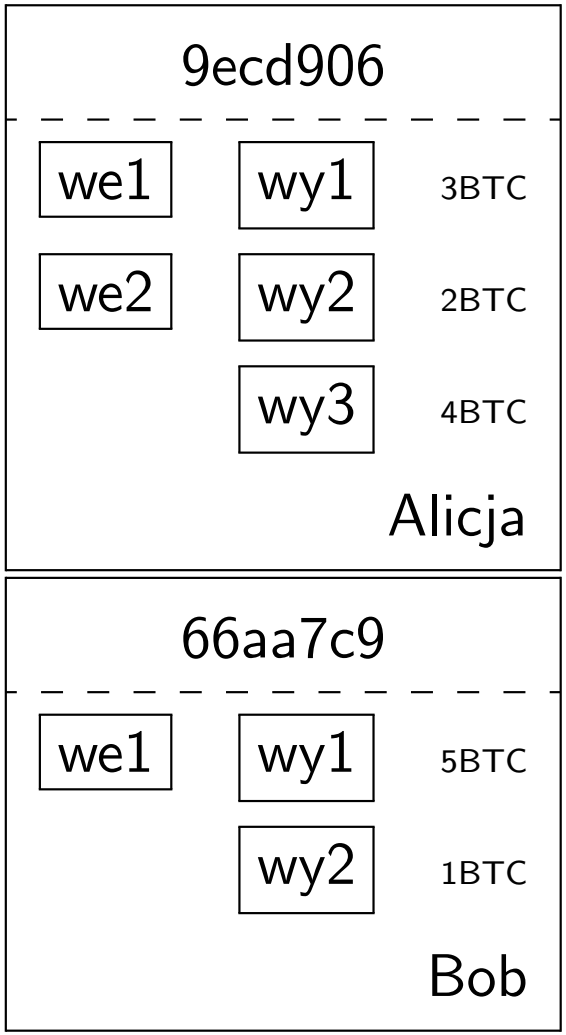
Transakcje

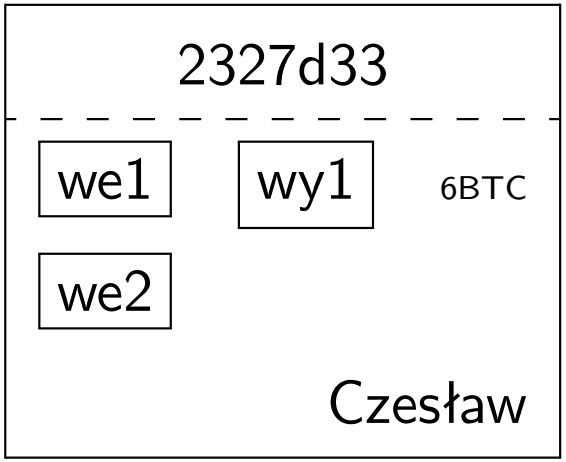


Transakcje

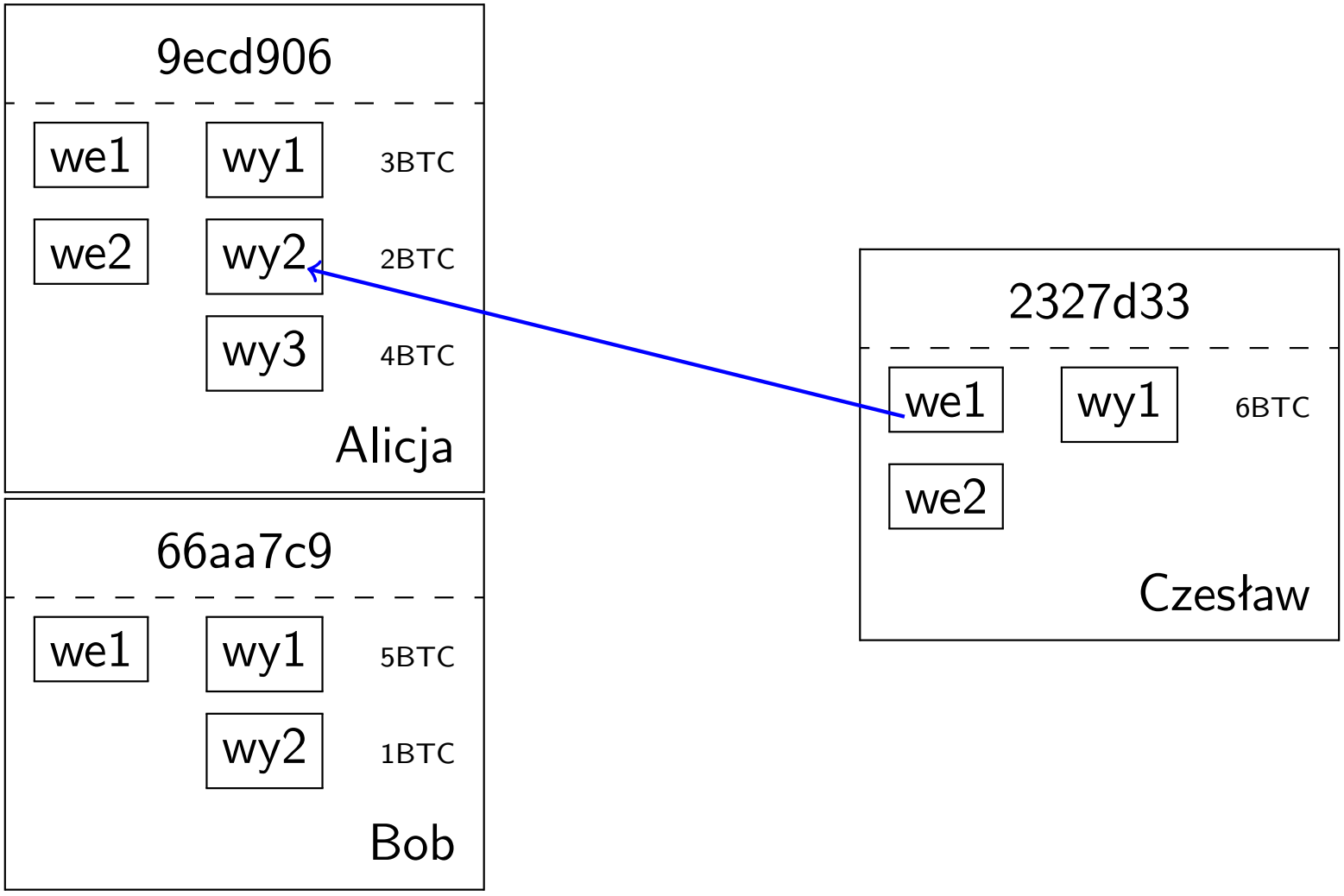

9ecd906
we1
wy1
3BTC
we2
wy2
2BTC
wy3
4BTC
Alicja
66aa7c9
we1
wy1
5BTC
wy2
1BTC
Bob

Transakcje

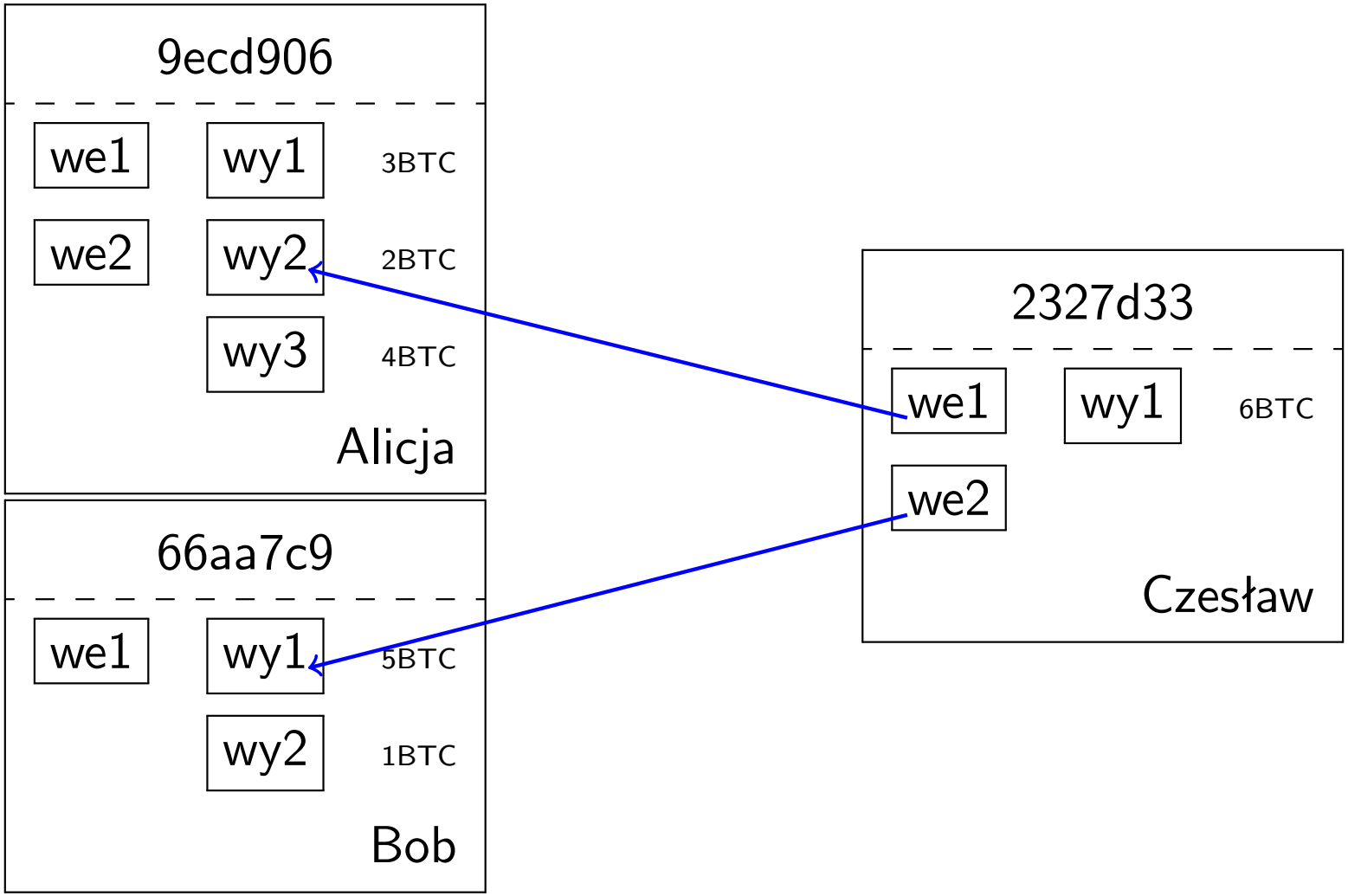

9ecd906
we1
wy1
3BTC
we2
wy2
2BTC
wy3
4BTC
Alicja
66aa7c9
we1
wy1
5BTC
wy2
1BTC
Bob


2327d33
we1
wy1
6BTC
we2
Czesław

Transakcje

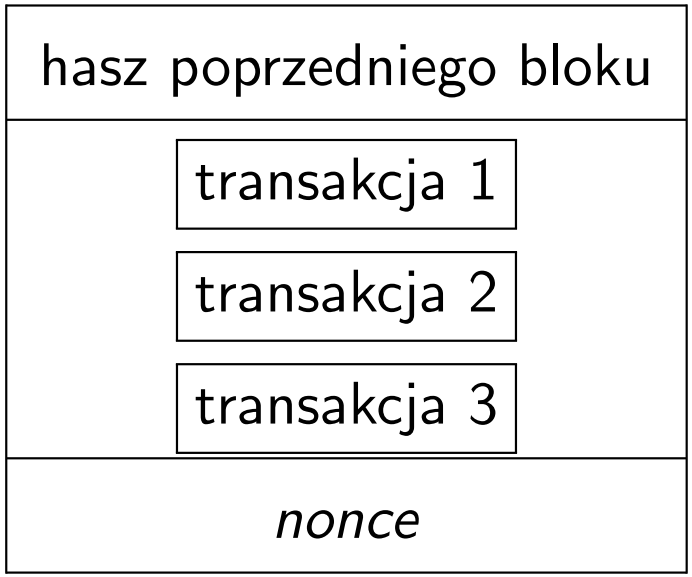

9ecd906
we1
wy1
3BTC
we2
wy2
2BTC
wy3
4BTC
Alicja
66aa7c9
we1
wy1
5BTC
wy2
1BTC
Bob
2327d33
we1
wy1
6BTC
we2
Czesław

Transakcje


9ecd906
we1
wy1
3BTC
we2
wy2
2BTC
wy3
4BTC
Alicja
66aa7c9
we1
wy1
5BTC
wy2
1BTC
Bob
2327d33
we1
wy1
6BTC
we2
Czesław

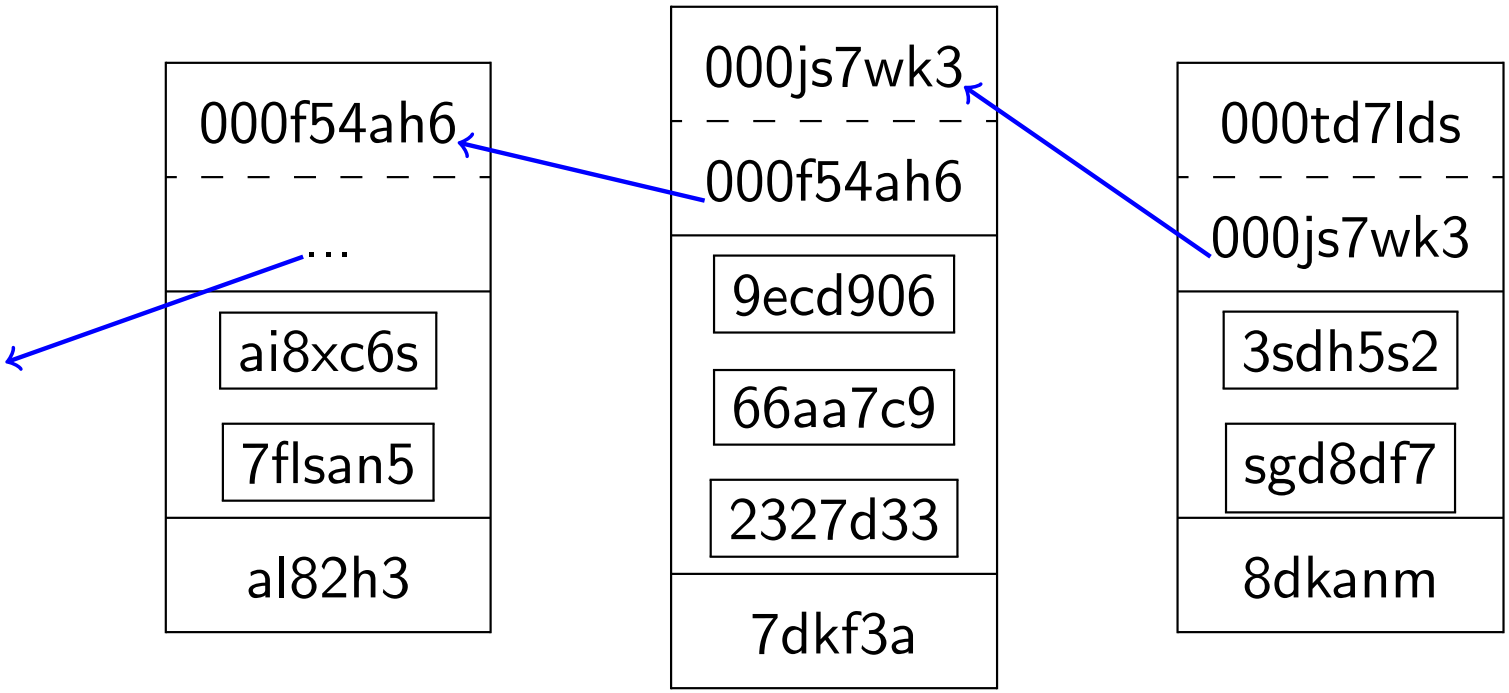
Blok

Blok

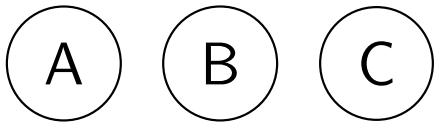

hasz poprzedniego bloku
transakcja 1
transakcja 2
transakcja 3
nonce

Łańcuch bloków

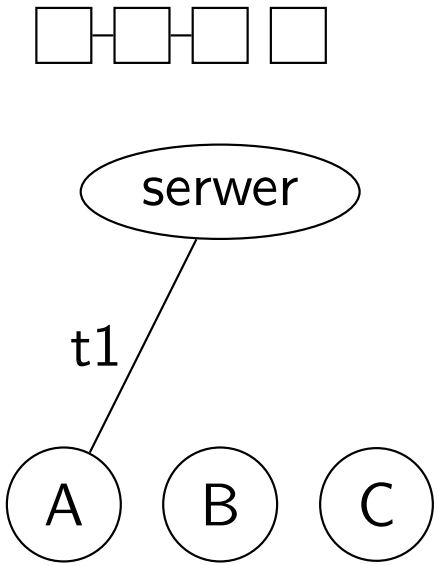
Łańcuch bloków



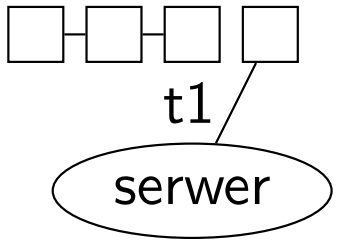
Symulacja działania

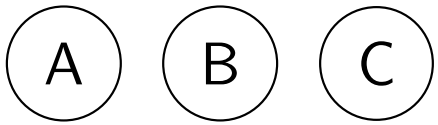


Symulacja działania

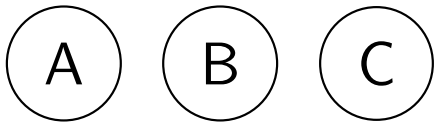


Symulacja działania

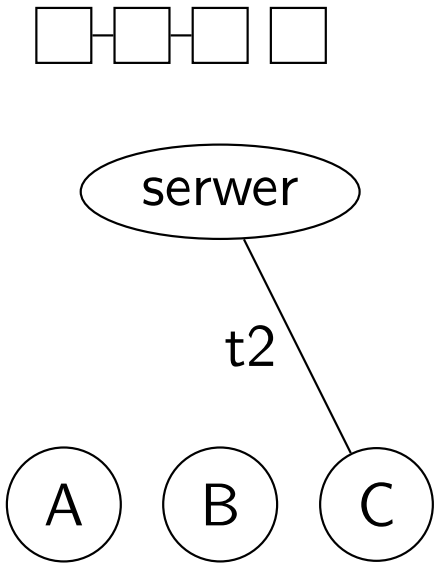




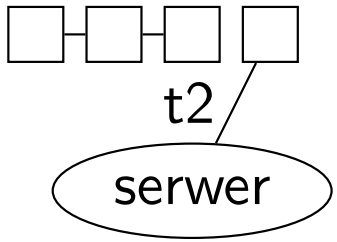
Symulacja działania

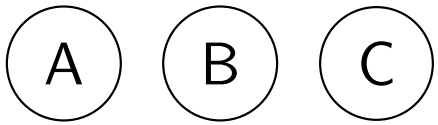


Symulacja działania

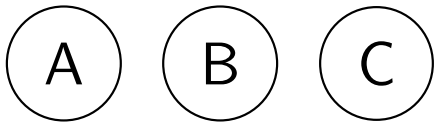


Symulacja działania

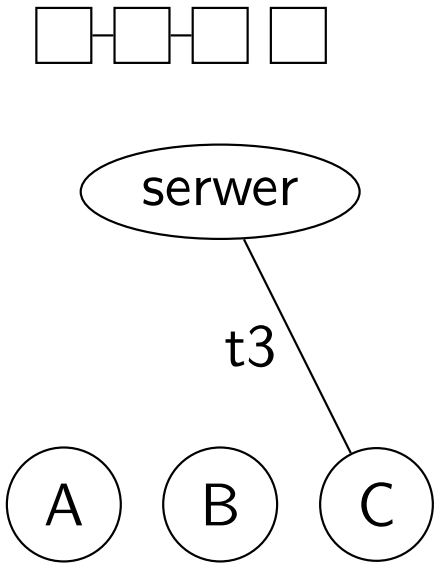




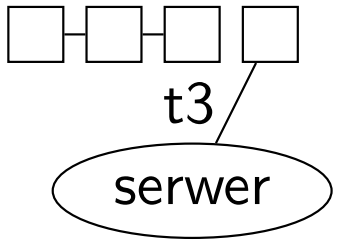
Symulacja działania

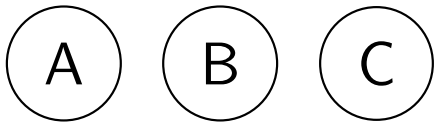


Symulacja działania

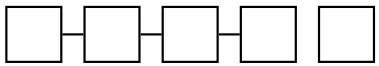


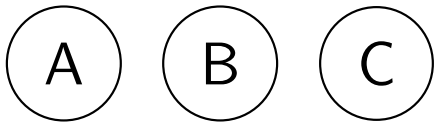
Symulacja działania



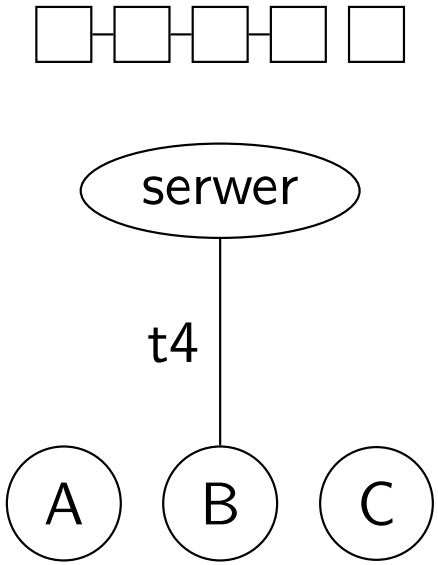


Symulacja działania

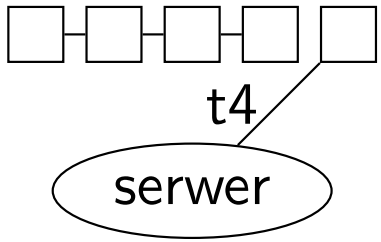


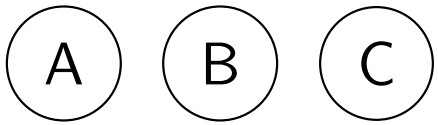


Symulacja działania

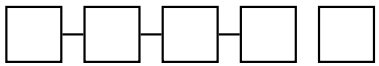


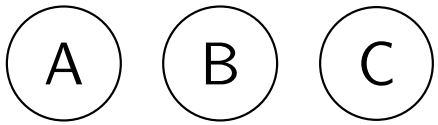
Symulacja działania



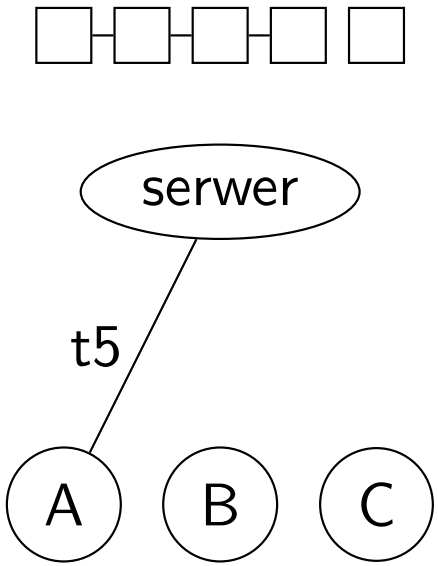


Symulacja działania

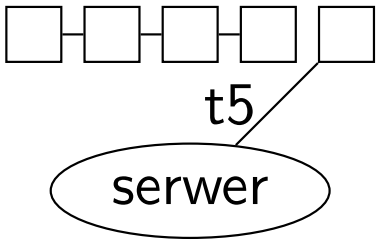


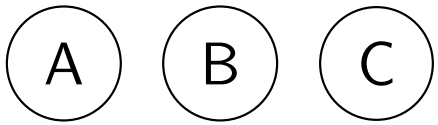


Symulacja działania

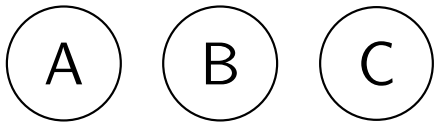


Symulacja działania





Symulacja działania



Blockchain po raz drugi

Jak pozbyć się centralizacji?

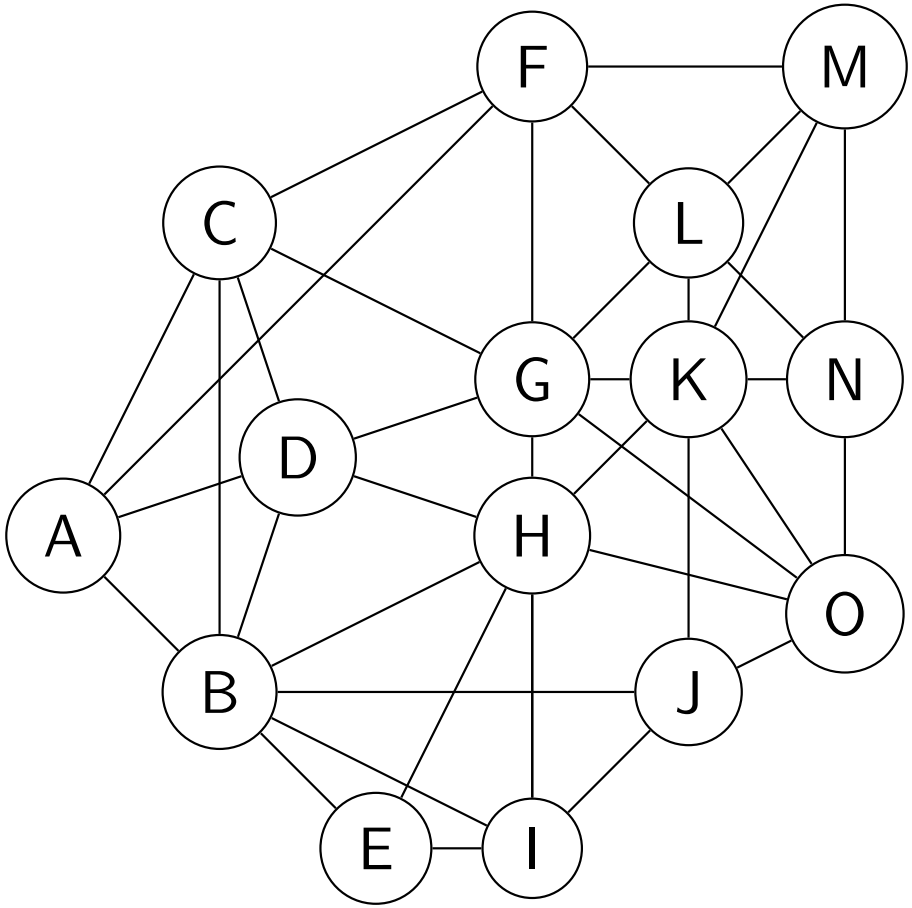
Jak pozbyć się centralizacji?

Sieć P2P

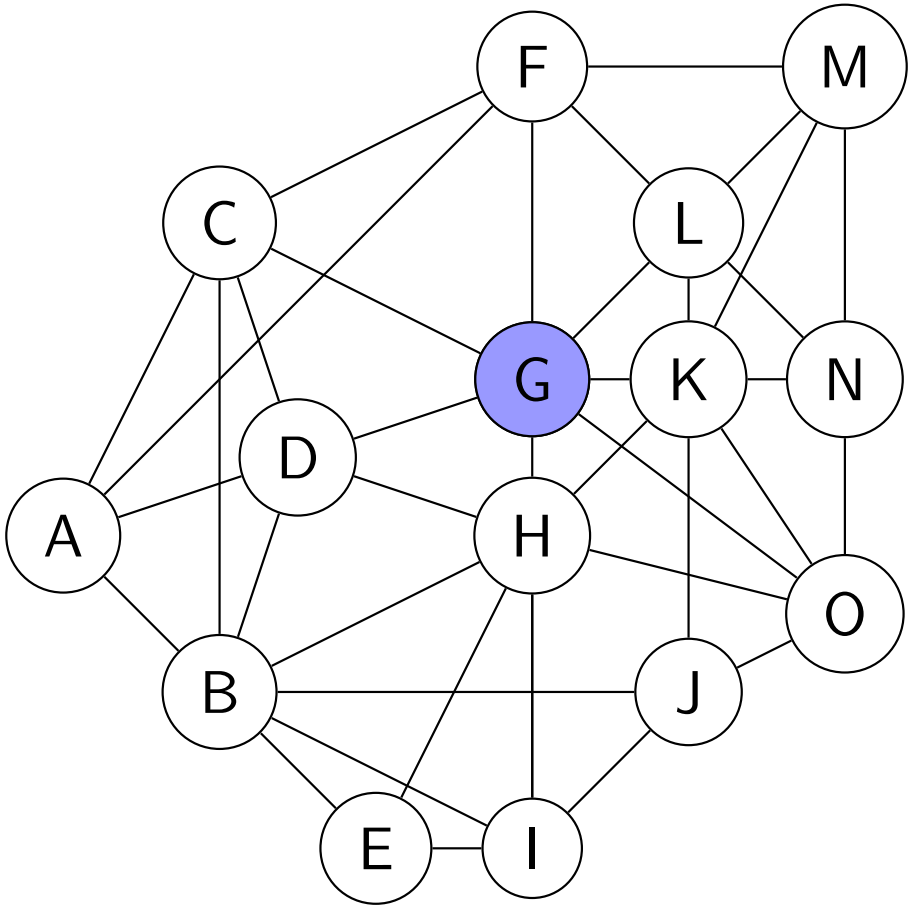
(ang. *peer-to-peer*)

P2P

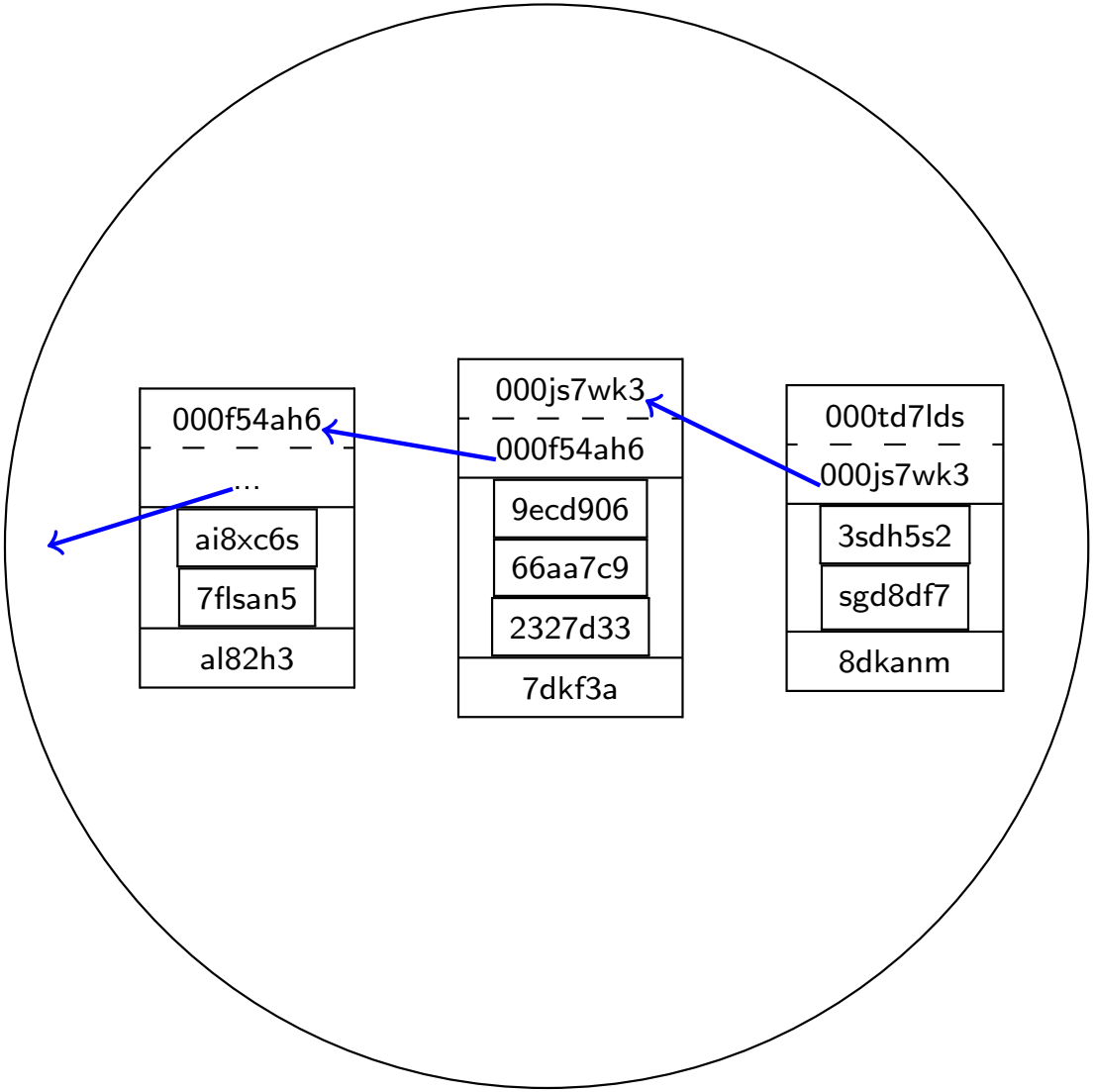
P2P



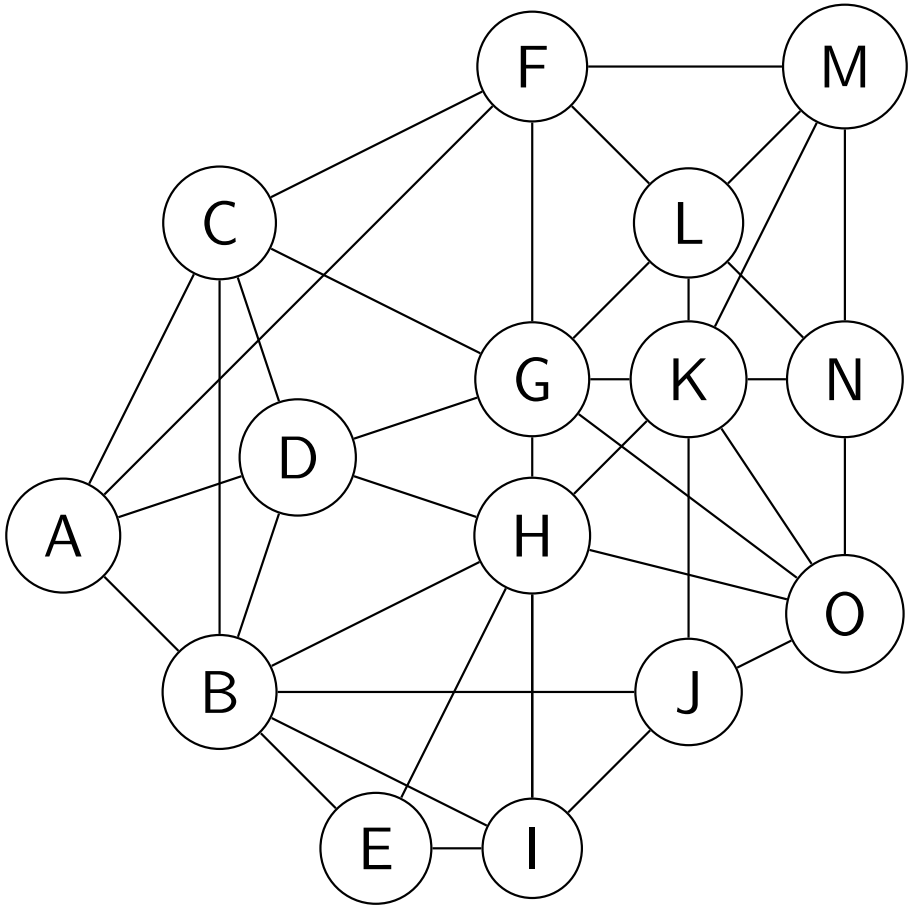
P2P



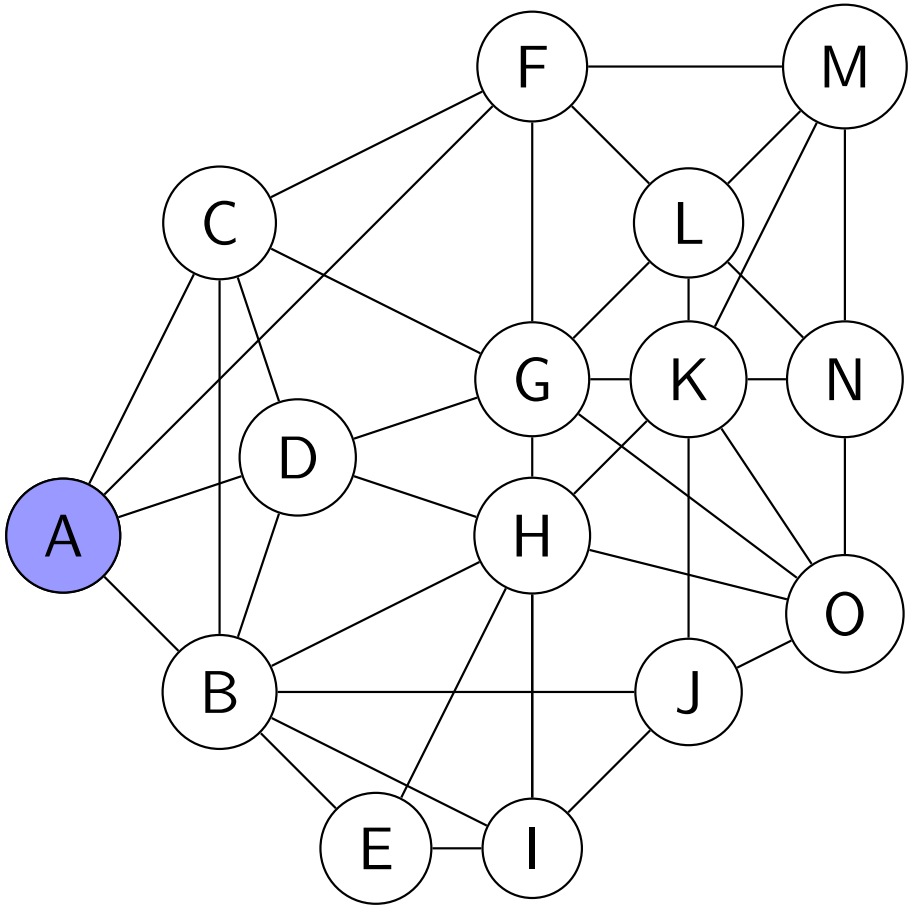
P2P


000f54ah6
...
ai8xc6s
7flsan5
al82h3
000js7wk3
000f54ah6
9ecd906
66aa7c9
2327d33
7dkf3a
000td7lds
000js7wk3
3sdh5s2
sgd8df7
8dkanm

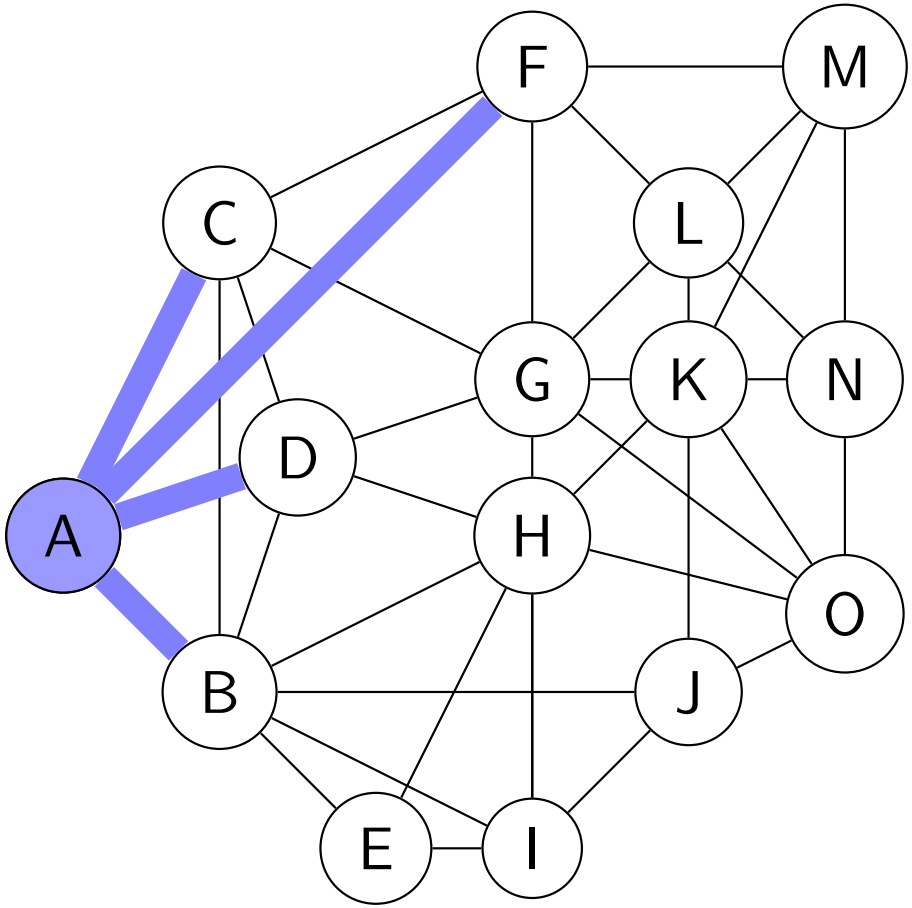
P2P



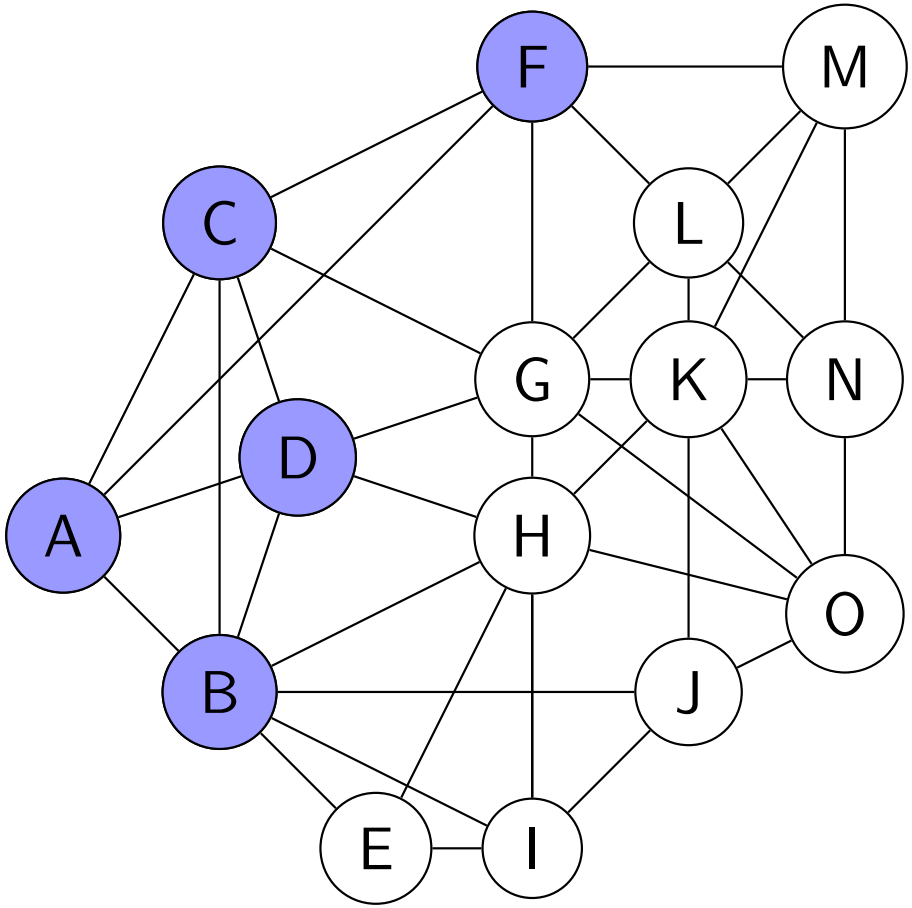
P2P



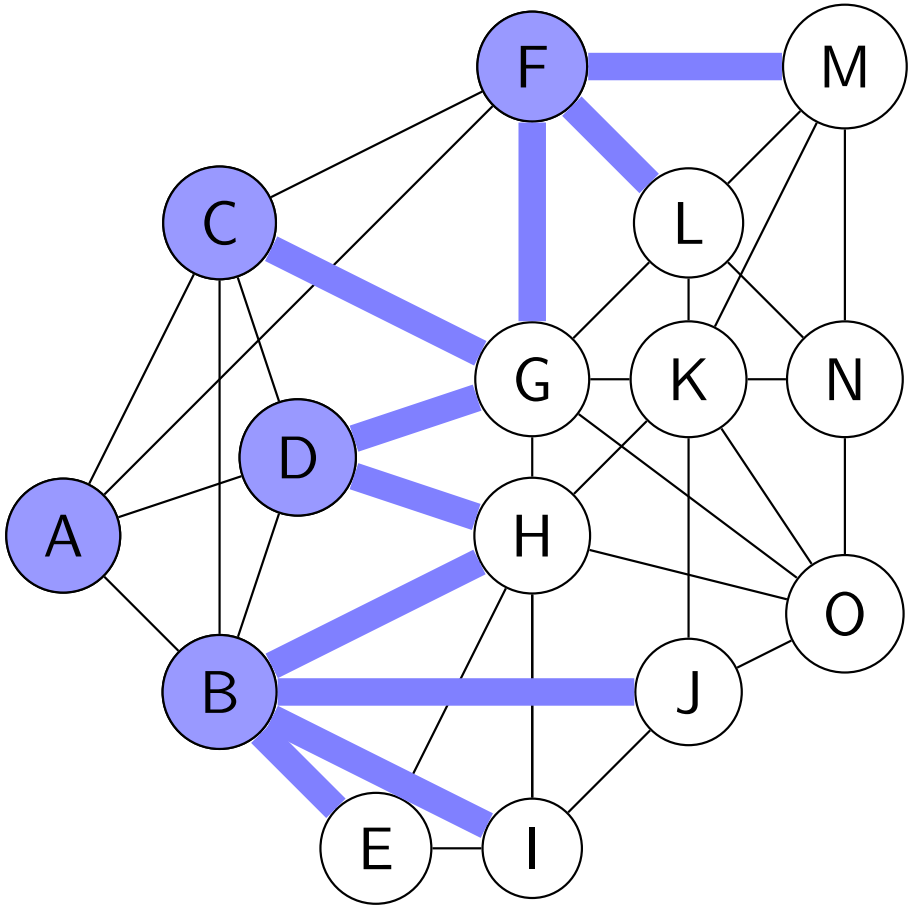
P2P



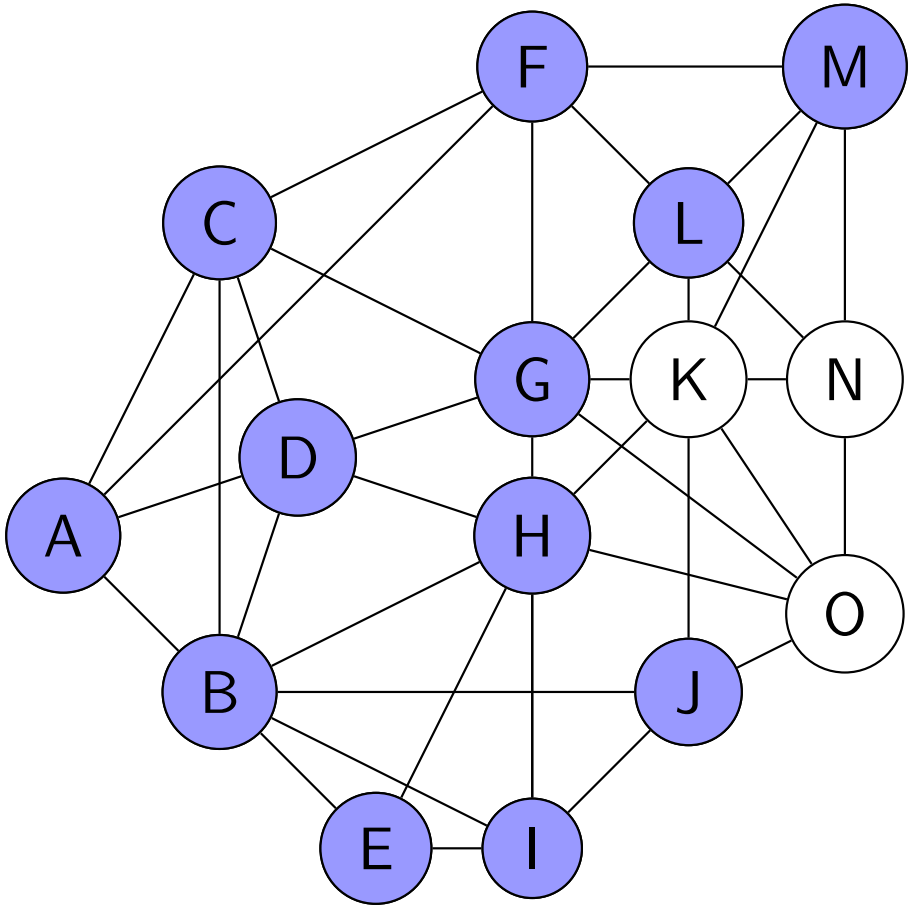
P2P



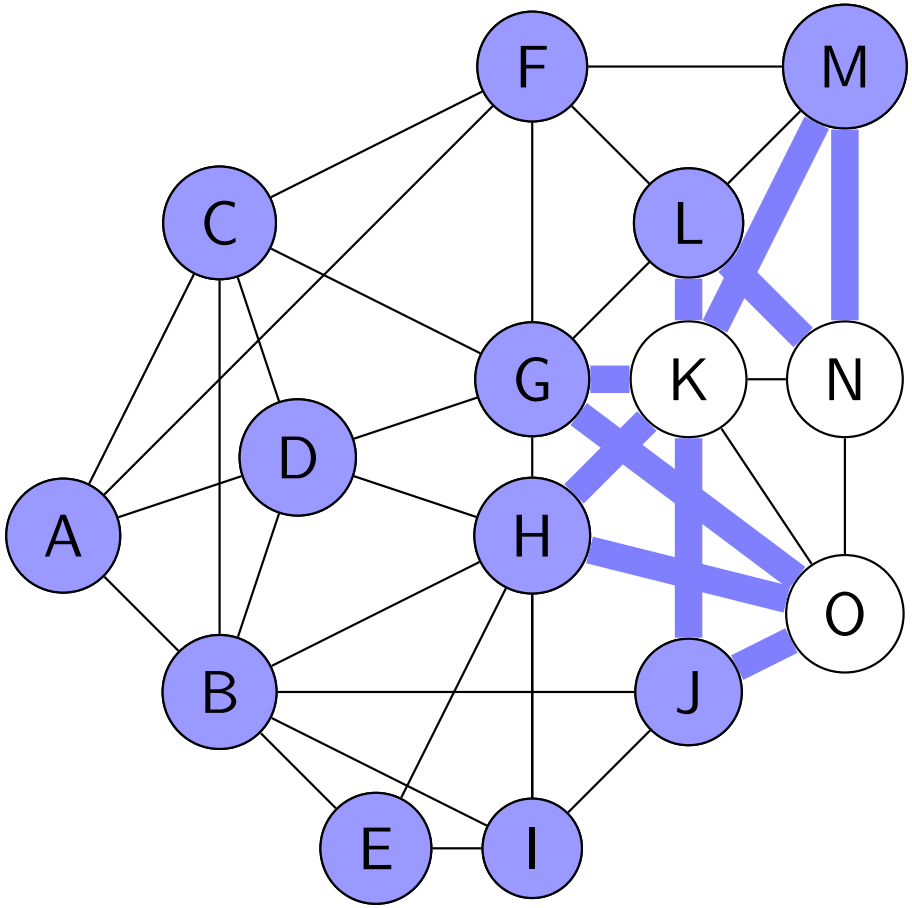
P2P



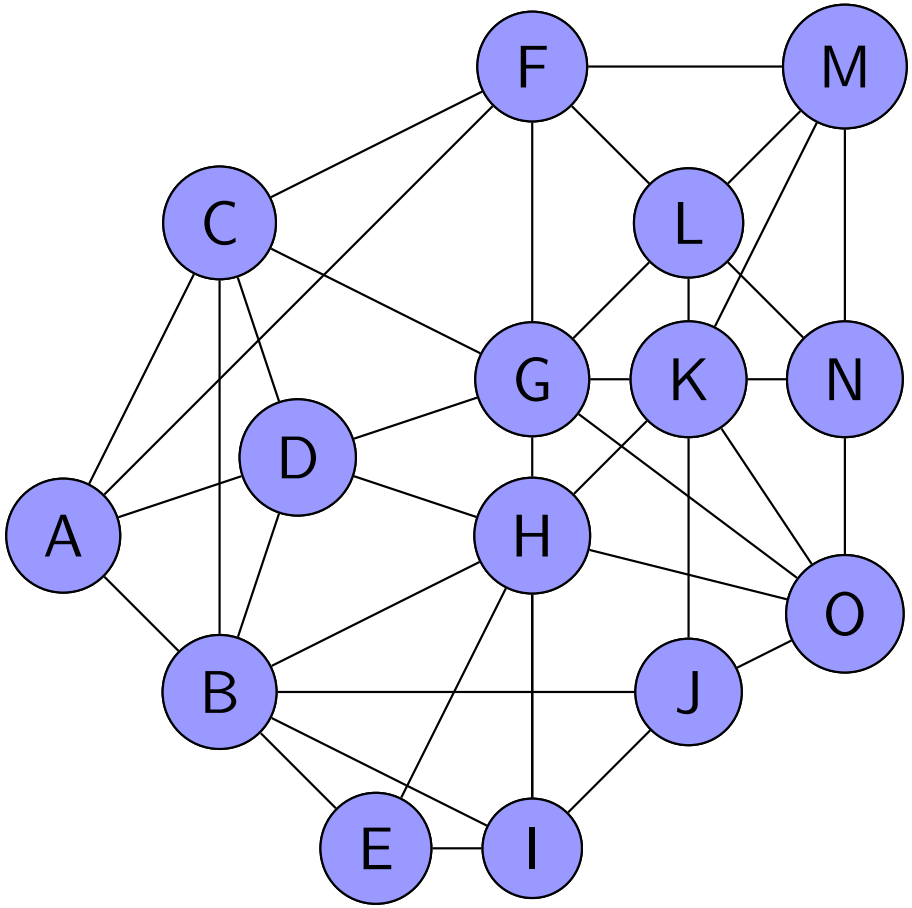
P2P



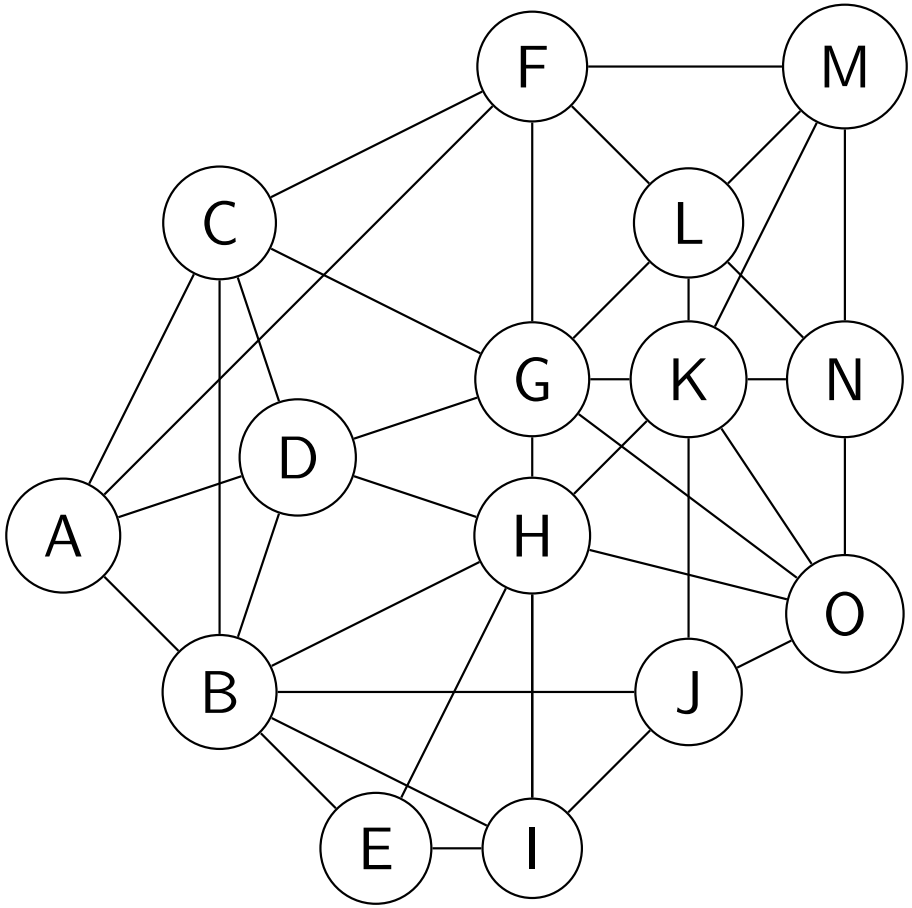
P2P



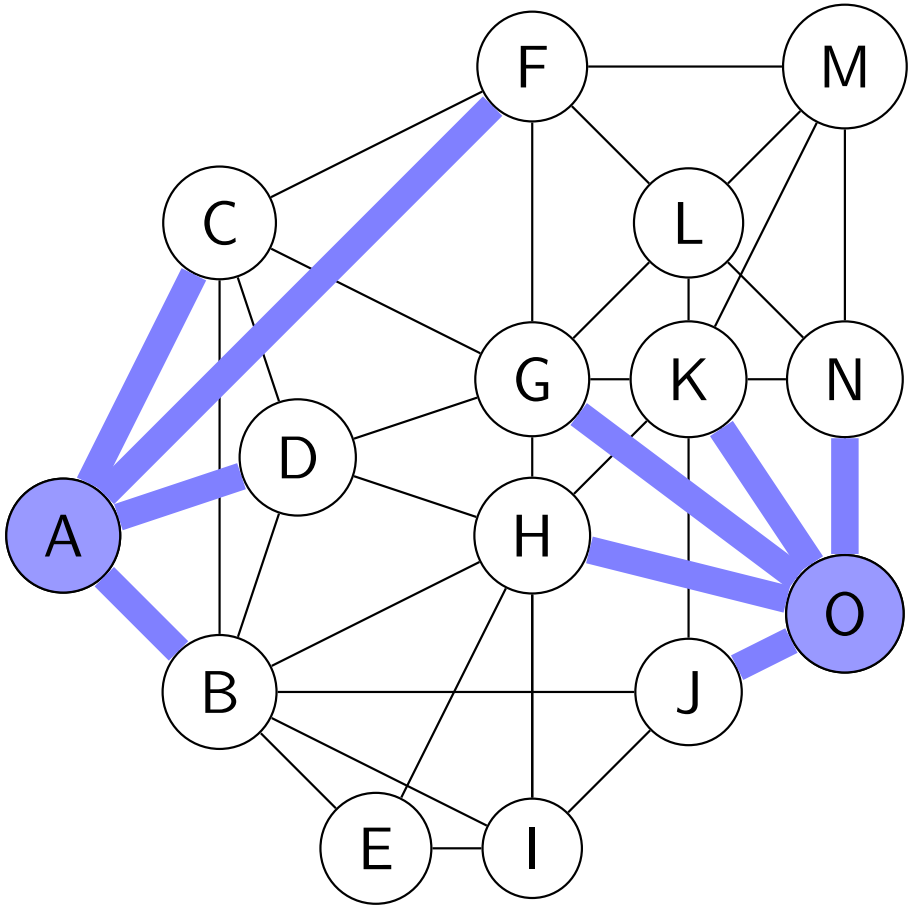
P2P



Co z równoczesnymi transakcjami?

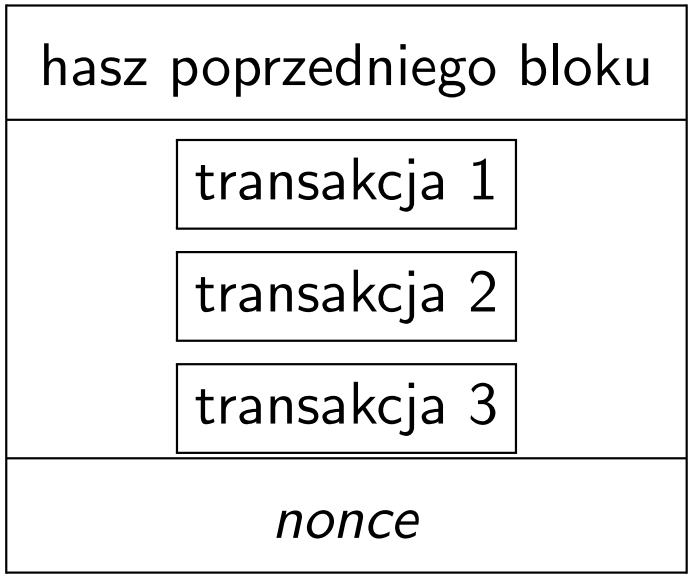


Co z równoczesnymi transakcjami?

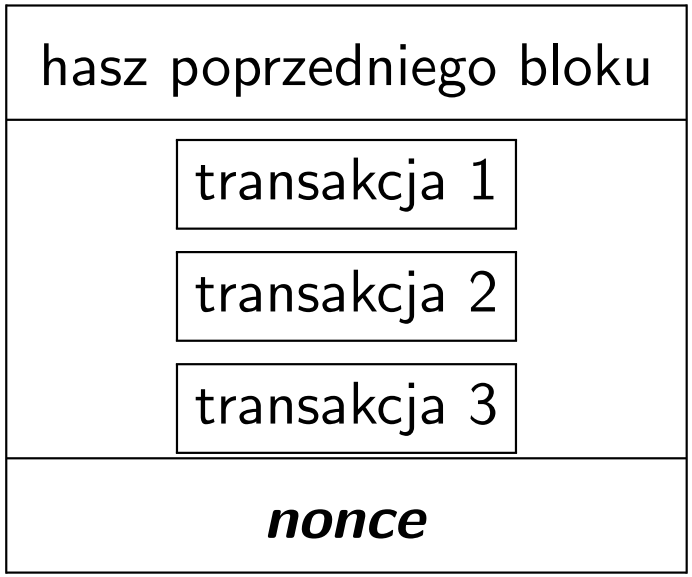


Proof of Work

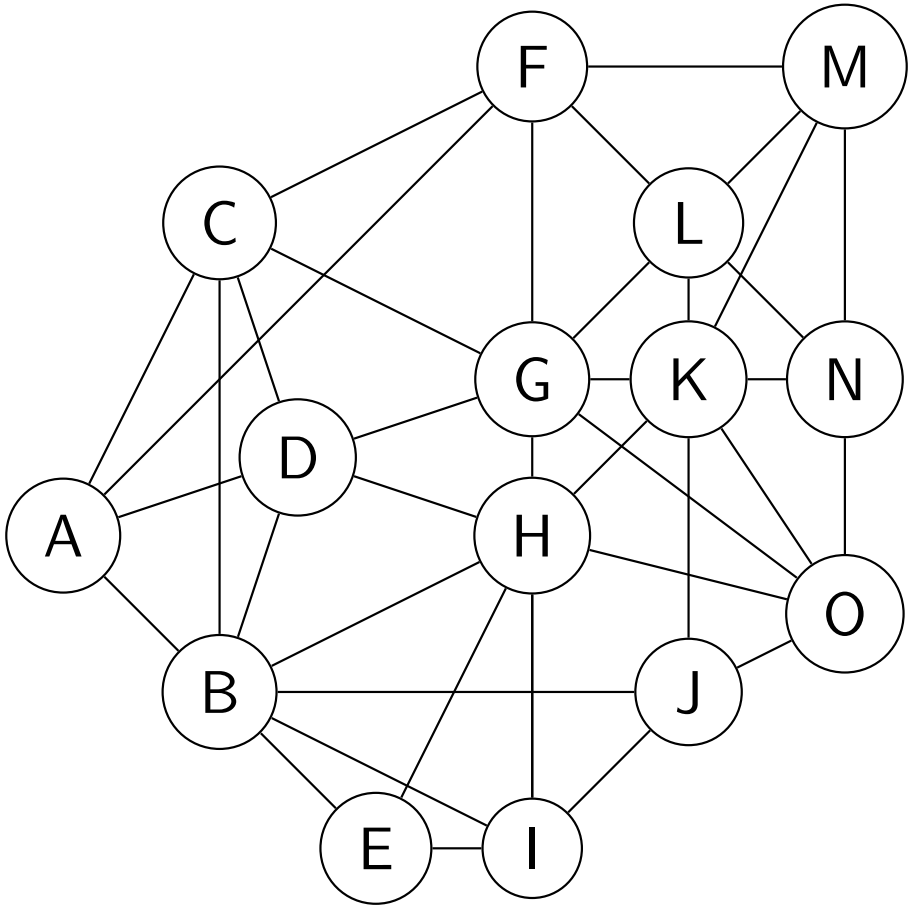
Proof of Work



Proof of Work



Proof of work



Co z innymi nierozwiązanymi blokami?

Co z innymi nierozwiązanymi blokami?

Są porzucane.

Co z innymi nierozwiązanymi blokami?

Są porzucane.

Dlaczego?

Co z innymi nierozwiązanymi blokami?

Są porzucane.

Dlaczego?

Zasada: wygrywa dłuższy łańcuch

Czy opłaca się „kopać”?

Czy opłaca się „kopać”?

Tak!

Czy opłaca się „kopać”?

Tak!

- opłaty transakcyjne

Czy opłaca się „kopać”?

Tak!

- opłaty transakcyjne
- nagroda - aktualnie generowane 12,5 BTC

Fakty i mity

Fakty i mity

- zmiany w blokach właściwie niemożliwe

Fakty i mity

- zmiany w blokach właściwie niemożliwe
- nie anonimowy, a przezroczysty

Fakty i mity

- zmiany w blokach właściwie niemożliwe
- nie anonimowy, a przezroczysty
- powolne potwierdzanie transakcji

Podsumowanie

Podsumowanie

Podsumowanie

- Hasz

Podsumowanie

- Hasz
- Szyfrowanie asymetryczne (klucz prywatny i publiczny)

Podsumowanie

- Hasz
- Szyfrowanie asymetryczne (klucz prywatny i publiczny)
- Transakcje i bloki

Podsumowanie

- Hasz
- Szyfrowanie asymetryczne (klucz prywatny i publiczny)
- Transakcje i bloki
- Blockchain

Podsumowanie

- Hasz
- Szyfrowanie asymetryczne (klucz prywatny i publiczny)
- Transakcje i bloki
- Blockchain
- P2P

Podsumowanie

- Hasz
- Szyfrowanie asymetryczne (klucz prywatny i publiczny)
- Transakcje i bloki
- Blockchain
- P2P
- Proof of Work

Dziękuję za uwagę!

Bitcoin i inne kryptowaluty

Jakub Cisło

Programowanie z pasją

http://cislo.net.pl

jakub@cislo.net.pl

25 maja 2018

Referencje

1. https://anders.com/blockchain/
2. https://anders.com/blockchain/public-private-keys/
3. https://en.bitcoin.it/wiki/Protocol_documentation
4. http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html
5. https://blockchain.info/
6. https://blockexplorer.com/
7. http://bitcoin.pl/